AMENDMENTS TO THE CLAIMS

Amended claims follow:

1. (Currently Amended) An apparatus for providing a security status of an on-line service, comprising:

a web page object that is automatically rendered by a browser when a visitor uses the browser to access one or more web pages of the on-line service via a public network; and

a verification service that hosts the web page object separately from the one or more web pages of the on-line service, and further controls contents of the web page object,

wherein the visitor is not required to take any action other than requesting access to the on-line service via the browser to receive the security status through the automatic rendering of the web page object by the visitor's browser, and

wherein the verification service causes the contents of the web page object to be changed in accordance with its prior determination of a level of the security status, such that when the verification service determines, in a first verification operation prior to the visitor's access request, that the on-line service has a first level of the security status, it causes the web page object to have first contents, and when the verification service determines, in a second verification operation prior to the visitor's access request, that the on-line service has a different second level of the security status, it causes the web page object to have different second contents, and thereby automatically controls the visitor's perception of the different security status levels via the browser's automatic rendering of the prior-determined and changed web page object contents when the visitor requests access to the on-line service, and

wherein the first and second verification operations to determine the on-line service's security status and control the contents of the web page object are performed by the verification service prior to and completely independently from the visitor's request to access the on-line service, and independently from any action by the visitor and the visitor's browser, and

wherein the levels of the security status displayed for the visitor via the automatic rendering of the web page object indicate how vulnerable devices and services of the on-line service are to hackers and other online security threats as determined by the first and second verification operations, and

wherein at least one of the first and second verification operations include determining the security status by comparing a fingerprint of a new vulnerability to a stored list of the devices and services and without performing an actual scan or test of the devices and services, and

wherein when the verification service causes the web page object to have at least one of the first and second contents, the web page object appears invisible to the visitor after it is rendered by the visitor's browser, and

wherein at least one of the first and second verification operations includes scanning the on-line service from a remote address on the network, and

wherein the scanning produces a set of XML files including information about open ports, available service, network protocols, security exposures and vulnerabilities associated with a device providing the on-line service, and

wherein a scan header record associated with the scanning is stored in a database, the scan header record including a date, launch time, duration and a number of vulnerabilities classified by severity level.

2. (Previously Presented) An apparatus according to claim 1, wherein the verification service determines the security status level of the on-line service by evaluating a vulnerability scan of the devices and services comprising the on-line service.

3-8. (Cancelled)

9. (Previously Presented) An apparatus according to claim 2, wherein the verification service periodically receives results of a new vulnerability scan of the devices and services comprising the on-line service and causes the contents of the web page object to be changed if a changed security status level is determined, thereby automatically providing the visitor with an updated security status.

10-20. (Cancelled)

21. (Currently Amended) A method for providing a security status of an on-line service, comprising:

hosting a web page object separately from one or more web pages of the on-line service;

providing a link to the web page object so that it is automatically rendered by a browser when a visitor uses the browser to access the one or more web pages of the on-line service via a public network;

providing an indication of the security status of the on-line service to the visitor via the automatic rendering of the web page object by the visitor's browser, wherein the visitor is not required to take any action other than requesting access to the on-line service via the browser to receive the security status; and

changing the contents of the web page object to be automatically rendered and displayed in accordance with a determination of a level of the security status, including:

in a first verification operation prior to the visitor's access request, causing the web page object to have first contents if the on-line service has a first level of the security status, and

in a second verification operation prior to the visitor's access request, causing the web page object to have different second contents if the on-line service has a different second level of the security status,

thereby automatically controlling the visitor's perception of the different security status levels via the browser's automatic rendering of the prior-determined web page object contents when the visitor requests access to the on-line service,

wherein the first and second verification operations to determine the on-line service's security status and control the contents of the web page object are performed prior to and completely independently from the visitor's request to access the on-line service, and independently from any action by the visitor and the visitor's browser, and

wherein the levels of the security status displayed for the visitor via the automatic rendering of the web page object indicate how vulnerable devices and services of the on-line service are to hackers and other online security threats as determined by the first and second verification operations, and

wherein at least one of the first and second verification operations include determining the security status by comparing a fingerprint of a new vulnerability to a stored list of the devices and services and without performing an actual scan or test of the devices and services, and

wherein, when the web page object is caused to have at least one of the first and second contents, the web page object appears invisible to the visitor after it is rendered by the visitor's browser, and

wherein at least one of the first and second verification operations includes scanning the on-line service from a remote address on the network, and

wherein the scanning produces a set of XML files including information about open ports, available service, network protocols, security exposures and vulnerabilities associated with a device providing the online service, and

wherein a scan header record associated with the scanning is stored in a database, the scan header record including a date, launch time, duration and a number of the vulnerabilities classified by severity level.

22-26. (Cancelled)

27. (Previously Presented) A method according to claim 21, wherein the first and second verification operations include determining the security status level of the on-line service by evaluating a vulnerability scan of the devices and services comprising the on-line service.

28. (Previously Presented) A method according to claim 27, further comprising periodically receiving results of a new vulnerability scan of the devices and services comprising the on-line service and causing the contents of the web page object to be

changed if a changed security status level is determined, thereby automatically providing the visitor with an updated security status.

29. (Previously Presented) A method according to claim 21, wherein the web page object comprises an image and an associated URL.

30. (Previously Presented) A method according to claim 21, wherein the web page object comprises a graphical file whose contents are periodically updated in accordance with a periodically determined security status level.

31-33. (Cancelled)

34. (New) An apparatus according to claim 1, wherein the database stores the information about the open ports on the device providing the online service, generic services expected to be running on the open ports, and actual services running on the open ports, including a version and network message protocol associated with the actual services.

35. (New) An apparatus according to claim 1, wherein the scanning is performed using a scanning engine of the verification service.

36. (New) An apparatus according to claim 35, wherein the scanning engine parses the set of XML files and stores records of the parsed set of XML files in the database in association with an account number of a provider of the online service.

37. (New) An apparatus according to claim 36, wherein the records include a detail record for each positive test result associated with the scanning.

38. (New) An apparatus according to claim 1, wherein the visitor is allowed to log in and review interactive reports associated with the scanning.

39. (New) An apparatus according to claim 1, wherein the levels of the security status displayed for the visitor include a security meter.

40. (New) An apparatus according to claim 1, wherein the levels of the security status displayed for the visitor include an overall numeric rating.

41. (New) An apparatus according to claim 1, wherein the scanning is performed according to a schedule.

42. (New) An apparatus according to claim 41, wherein the schedule is requested by the visitor.

43. (New) An apparatus according to claim 1, wherein information in the database is initialized manually.

44. (New) An apparatus according to claim 1, wherein information in the database is initialized automatically.

45. (New) An apparatus according to claim 1, wherein the scanning is performed on each device registered by the on-line service in the database.